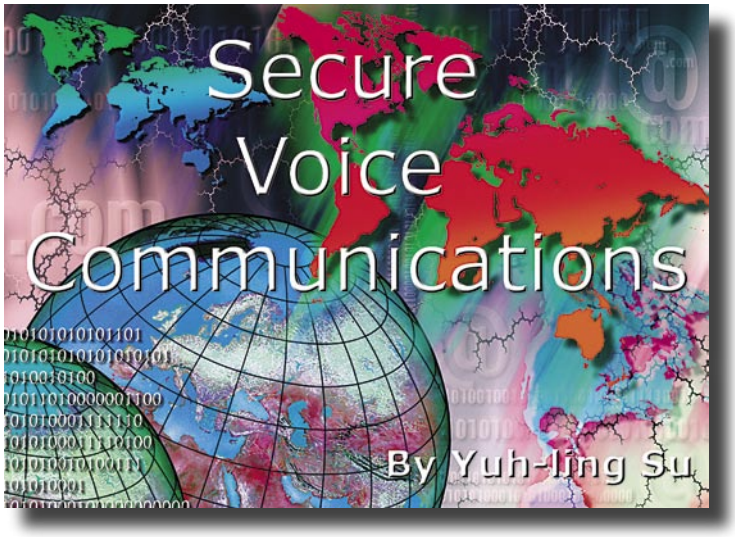

The need for secure data and secure voice is increasing dramatically with new threats and the global war on terrorism …

Military units require a full spectrum of communications capabilities to ensure that all elements of command and control (C2), *(battle orders, planning, logistics, medical, personnel, etc.)* are communicated effectively. Secure communication systems may be considered the lifeline of C2 on the battlefield and must be available to U.S. forces at all levels, from strategic to tactical.

FORCEnet will enable the integration of secure voice with data and sensor networks within the Global Information Grid (GIG). Integration of secure voice within FORCEnet is enabled by the rapidly maturing Voice over Internet Protocol (VoIP). In the last decade, circuit-switched technologies (used for voice communications) are transitioning to packet-switched integrated networks that support both data and voice.

The need for secure data and secure voice is increasing dramatically with new threats and the global war on terrorism. Today's warfighter must be able to use both secure voice and secure data simultaneously for effective collaboration. The future of end-to-end secure communications will be driven by Department of Defense (DoD) requirements, including joint and coalition collaboration, and the growing need to interoperate through the full range of federated operations involving U.S. government organizations such as the Department of Homeland Security, state and local government and others as directed. The convergence of voice and data in secure VoIP is a cost-effective enabler for these missions.

The Navy Secure Voice Team of the PEO C4I and Space, PMW 160, with technical expertise from SPAWAR Systems Center San Diego Code 2877, St. Julien's Creek, Va., is developing the Naval Advanced Secure Voice Architecture (NASVA) that identifies the future of secure voice communications in the sea, land and air warfare missions of the Department of the Navy. The NASVA describes an acquisition process that will leverage the spiral development process. It also provides the guidance necessary to integrate policies, requirements and technologies to successfully move from today's "as is" architecture to the future "to be" secure voice architecture.

The Secure Voice Team will leverage industry technologies and innovations, and rely on a comprehensive assessment of capabilities required by users. The team will also conduct continuous, in-depth examinations of emerging technologies that may deliver those capabilities. It is hoped that this approach will energize the development of technology to achieve immediate gains in capability under a rapid insertion scenario.

The Navy secure voice team is using a four-pronged approach to capture user requirements and help guide development efforts to meet users' needs:

√ Review the Joint Mission Essential Task List (JMETL) and Naval Mission Essential Task List (NMETL) to determine documented requirements.

√ Develop a Web-based questionnaire for recently deployed fleet, Marine Corps, joint and special warfare forces to collect a continuing flow of anecdotal or empirical information about equipment and user desired improvements or features.

√ Follow up with interviews of returning strike groups and special warfare units to capture the "real story" of system performance and solicit new ideas. Candid feedback to the online survey and fleet liaison visits are critical to the collection and analysis of requirements.

√ Consult industry to leverage emerging communications and network technologies. Selected technologies will be tested during Sea Trial events (*e.g., Trident Warrior series exercises)* for suitability.

Requirements gathering starts below decks with interior communications systems and extends through the "last mile" all the way to the "foxhole" in support of Army and Marine Corps units. The Secure Voice Team is investigating the full spectrum of technologies with an eye toward future net-centric requirements.

Major technological issues, technology mandates, security concerns, and integration and interoperability requirements all provide a catalyst for close partnership with industry to produce the next generation of secure communication devices.

The technological challenges of secure voice integration are many and complex. The convergence of voice and data presents a significant challenge for the prioritization of packets and managing traffic flow over an IP network while also meeting the quality of service requirements for voice, combat systems and other mission critical systems.

Interoperability issues are driven by DoD mandates, compelling the adoption of new features or security schemata that can cause interoperability problems (in particular with legacy

equipment). For instance, the Joint Tactical Radio System has been mandated as the joint standard for the future of radio frequency (RF) communications in DoD, and secure voice devices must accommodate this emerging standard. Another mandate is for IP migration to an IPv6 capable architecture for all communications and data systems by 2008.

In order to meet the net-centric secure voice requirements, the Secure Voice Team is pressing for the following initiatives:

√ Secure Communication Interoperability Protocol *(SCIP, previously known as Future Narrowband Digital Terminal, FNBDT)* Voice Gateway compresses voice signals to enable transmission over tactical links. This gateway is crucial to ships underway due to limited bandwidth on the battlefield and aboard ship.

Voice is critical for reach back to headquarters and remote medical and technical expertise — even more critical as manpower is reduced. In addition, the SCIP Voice Gateway will convert traditional telephony voice into IP packets that can be routed by the Advanced Digital Network System from and to the tactical links, maximizing use of available tactical bandwidth rather than requiring dedicated voice links.

√ Variable Data Rate (VDR) Voice Encoder enables 28 instantaneous data rates (2.4 kbps to 32 kbps) to optimize use of IP bandwidth while maintaining voice quality. It also provides narrowband to wideband interoperability. The dynamic VDR arbitrator enables the VDR voice encoder to set the data rate on the fly based on the network traffic conditions.

√ Secure Voice Core Technology supports voice encoding, encryption and instantaneous variability (using VDR) over a wide range of data rates, ensuring best voice quality over a challenged network. The encryption will include Type-1 and Advanced Encryption Standard (AES) algorithms.

√ Universal Voice Terminal (UVT) is a multifunctional, software configurable voice terminal that uses Secure Voice Core Technology. It will interface with VoIP and telephony systems, support new waveforms to meet future requirements, be compatible with existing RF components, and interoperate with legacy equipment via gateways. Land-based UVT can be used as a relay hub for the Personal Secure Telephone to provide worldwide secure voice coverage. The UVT could replace all current tactical secure voice crypto devices, dramatically reducing integrated logistics support, training and maintenance costs.

√ Personal Secure Telephone (PST) is a small, lightweight, multimedia, rugged, handheld wireless terminal that uses Secure Voice Core Technology. It will provide short-range tactical secure voice communications, interface with the UVT to extend tactical secure voice over the horizon and provide the Global Positioning System (GPS) reporting and targeting. Furthermore, the PST will use access controls, biometrics and a personal identification number (PIN) for authorization and authentication.

An important lesson learned from Operation Iraqi Freedom was that many situations preclude the use of Type-1 devices, and that the Navy required a small, wireless AES device for secure communications. A device supporting both Type-1 and AES encryption can also be used for DoD and homeland defense first-responder personnel.

A comprehensive secure voice architecture, well-defined fleet requirements, industry involvement and implementation of the secure voice initiatives are essential to ensure the superiority of secure voice communications …

√ Tactical Shore Gateway (TSG) is being installed at Naval Computer Telecommunications Area Master Stations to provide wireline/wireless telephone to tactical radio interoperability.

√ TSG for VoIP interoperability will combine the TSG and VoIP systems to provide an interface to an external connection that merges legacy secure voice systems, commercial telephony systems and IP networks with a tactical capability for Secure Voice over IP (SVoIP). This effort paves the way for tactical SVoIP capability, the first step toward integrating legacy secure voice systems and modern commercial telephony.

A comprehensive secure voice architecture, well-defined fleet requirements, industry involvement and implementation of the secure voice initiatives are essential to ensure the superiority of secure voice communications. Furthermore, benefits extend beyond the Navy, supporting the joint services and homeland defense missions.

Secure voice technologies will continue to evolve to integrate voice and data within FORCEnet into the GIG. Implementation of the planned architecture described in the Naval Advanced Secure Voice Architecture will extend superior situational awareness, which is heavily dependent on secure voice and data — all the way to the tactical edge.

The PEO C4I & Space, Networks, Information Assurance and Enterprise Services Program Office (PMW 160) provides all common network services and commodities used by multiple programs. PMW 160 consolidates network services in all classified domains to support cross-domain and coalition operations.

For more information about the PEO C4I & Space go to the SPAWAR home page at http://enterprise.spawar.navy.mil/.

Yuh-ling Su is the assistant program manager for the Navy Secure Voice Team (PEO C4I & Space, PMW 160).

CHIPS